世界知的所有権機関
国　際　事　務　局

PCT

# 特許協力条約に基づいて公開された国際出願

(51) 国際特許分類7
H04L 9/30, 9/08, G09C 1/00

A1

(11) 国際公開番号 WO00/45548

(43) 国際公開日 2000年8月3日(03.08.00)

(21) 国際出願番号 PCT/JP00/00475

(22) 国際出願日 2000年1月28日(28.01.00)

(30) 優先権データ

| | | |
|---|---|---|
| 特願平11/21254 | 1999年1月29日(29.01.99) | JP |
| 特願平11/239177 | 1999年8月26日(26.08.99) | JP |

(81) 指定国　AU, CN, JP, SG, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE)

添付公開書類
国際調査報告書

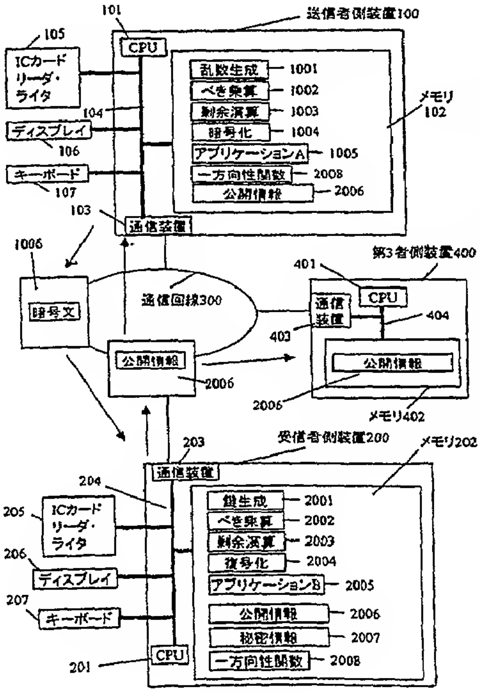
(71) 出願人（米国を除くすべての指定国について）
株式会社 日立製作所(HITACHI, LTD.)[JP/JP]
〒101-8010 東京都千代田区神田駿河台四丁目6番地
Tokyo, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
西岡玄次(NISHIOKA, Mototsugu)[JP/JP]
〒215-0013 神奈川県川崎市麻生区王禅寺1099番地
株式会社 日立製作所 システム開発研究所内 Kanagawa, (JP)
(74) 代理人
弁理士　作田康夫(SAKUTA, Yasuo)
〒100-8220 東京都千代田区丸の内一丁目5番1号
株式会社 日立製作所内 Tokyo, (JP)

## (54)Title: PUBLIC KEY CRYPTOGRAPH AND KEY SHARING METHOD

## (54)発明の名称　公開鍵暗号及び鍵共有方法

## (57) Abstract

A cryptograph communication method using public key cryptograph in which a sender creates a cryptogram by using a public key of the receiver by means of a sender device (100) and transmits it to the receiver device (200) through a communication line (300), and the receiver decrypts the cryptogram by using a secret key, wherein a procedure for encryption and decryption is so established to provide the features of security both the Rabin cryptograph which is one-way against chosen-plaintext attacks on the condition of difficulty of the problem of fractionization into prime factors and the ElGamal cryptograph which is strongly secret against chosen plaintext attacks on the condition of difficulty of the problem of Diffie-Hellman determination. Further while keeping secret the true plaintext space, the size of the plaintext space is reduced in order to use the space for key delivery of common key cryptogram. Thus a public key encrypting method and a key sharing method using the same are provided in which it is possible to prove the security on the condition of the problem more difficult than conventional, and high efficiency processing in the calculation for encryption/decryption is possible.



105...IC CARD READER/WRITER
106...DISPLAY
107...KEYBOARD
100...SENDER DEVICE
1001...RANDOM NUMBER GENERATION
1002...EXPONENTIATION
1003...REMAINDER CALCULATION
1004...ENCRYPTION
1005...APPLICATION A
2008...ONE-WAY FUNCTION
2006...PUBLIC INFORMATION
102...MEMORY
103...COMMUNICATION DEVICE
1006...CRYPTOGRAM
2006...PUBLIC INFORMATION
300...COMMUNICATION LINE
400...THIRD-PARTY DEVICE
403...COMMUNICATION DEVICE
2006...PUBLIC INFORMATION
402...MEMORY
205...IC CARD READER/WRITER
206...DISPLAY
207...KEYBOARD
203...COMMUNICATION DEVICE
200...RECEIVER DEVICE
202...MEMORY
2001...KEY GENERATION
2002...EXPONENTIATION
2003...REMAINDER CALCULATION
2004...DECRYPTION
2005...APPLICATION B
2006...PUBLIC INFORMATION
2007...SECRET INFORMATION
2008...ONE-WAY FUNCTION